

(19) 日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11) 特許出願公開番号

特開平10-336745

(43) 公開日 平成10年(1998)12月18日

(51) Int.Cl.⁶

識別記号

F I

H 0 4 Q 7/38

H 0 4 B 7/26

1 0 9 R

H 0 4 L 9/08

H 0 4 L 9/00

1 0 9 H

6 0 1 A

6 0 1 B

6 0 1 E

審査請求 有 請求項の数 6 O L (全 13 頁) 最終頁に続く

(21) 出願番号

特願平9-142681

(22) 出願日

平成9年(1997)5月30日

(71) 出願人 000004237

日本電気株式会社

東京都港区芝五丁目7番1号

(72) 発明者 大津 敏雄

東京都港区芝五丁目7番1号 日本電気株式会社内

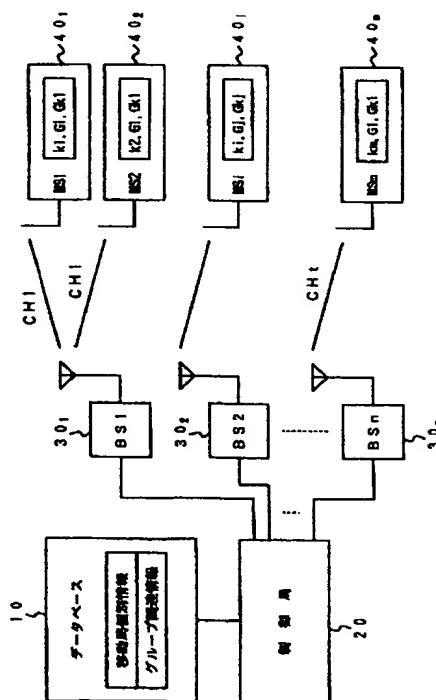
(74) 代理人 弁理士 後藤 洋介 (外2名)

(54) 【発明の名称】 移動通信システム

(57) 【要約】

【課題】 グループ構成の変更が安全且つ容易に可能なグループ秘話通信を行う移動通信システムを提供すること。

【解決手段】 この移動通信システムでは、制御局20により基地局(BS1~BSn)30₁~30_n及び移動局(MS1~MSm)40₁~40_m間での通信制御に際して使用するデータベース10に移動局個別情報を内部のマスタ鍵で暗号化して記憶すると共に、グループ関連情報を移動局個別の秘密鍵k_iで暗号化した情報を記憶し、システム内で使用する秘話通信の鍵を安全に記憶管理する。制御局20では同一グループに所属するそれぞれの移動局へのグループ暗号通信用秘密鍵Gk_iの配送時に配送先局の個別秘密鍵k_iで暗号化した情報を配送することにより、排他的なグループ秘話通信を安全且つ容易に実行する。



【特許請求の範囲】

【請求項1】 呼接続を含む通信制御に必要な通信制御情報を記憶するデータベースと、前記通信制御情報に基づいて通信制御を行う制御局とを備えると共に、該制御局の通信制御に従って無線回線を介してそれぞれ複数の基地局と複数の移動局とを組み合わせることで通信接続することにより、該複数の移動局間でグループを構成して排他的なグループ秘話通信が可能な移動通信システムであって、前記データベースは、移動局個別情報として移動局個別の秘密鍵を内部のマスタ鍵で暗号化して記憶すると共に、グループ関連情報として所属移動局毎にグループ内で共有するグループ暗号通信用秘密鍵を該移動局個別の秘密鍵で暗号化して記憶し、前記制御局は、新規にグループ構成が行われる毎に該グループに所属する移動局に対して前記暗号化したグループ暗号通信用秘密鍵を配送し、前記複数の移動局は、前記データベースに記憶されている前記移動局個別の秘密鍵のうちの自局用の秘密鍵を記憶すると共に、該秘密鍵を用いて前記制御局より配送された前記暗号化されたグループ暗号通信用秘密鍵を復号化した上、該復号化されたグループのうちの共有するグループ暗号通信用秘密鍵を用いてグループ通信情報を暗号化、復号化することを特徴とする移動通信システム。

【請求項2】 請求項1記載の移動通信システムにおいて、前記複数の移動局は、それぞれ自局の動作状態を前記複数の基地局のうちの特定のものと及び前記制御局を介して前記データベースへ通報し、前記データベースは、通報された前記複数の移動局のそれぞれの動作状態情報を前記移動局個別情報として記憶し、前記制御局は、前記グループ暗号通信用秘密鍵の配送時に該秘密鍵を受信不能であった該グループ所属の移動局が受信可能状態になった場合、該グループ暗号通信用秘密鍵として前記データベースにおける前記移動局個別情報に従って該移動局の秘密鍵で暗号化されたものを配送することを特徴とする移動通信システム。

【請求項3】 請求項1又は2記載の移動通信システムにおいて、前記データベースは、前記グループ暗号通信用秘密鍵として同一グループ内で共有するものを定期的に更新管理することを特徴とする移動通信システム。

【請求項4】 請求項1～3の何れか一つに記載の移動通信システムにおいて、前記データベースは、既設グループに所属移動局の追加を行う場合、該グループへの新規加入移動局の個別移動局情報として記憶されている該移動局の個別秘密鍵で該グループのうちの共有するグループ暗号通信用秘密鍵を暗号化してグループ関連情報として記憶し、且つ該グループ暗号通信用秘密鍵を前記制御局及び前記複数の基地局のうちの対応するものを介して配送することを特徴とする移動通信システム。

【請求項5】 請求項1～3の何れか一つに記載の移動通信システムにおいて、前記データベースは、既設グル

ープに所属移動局の一部削除を行う場合、該グループ関連情報より削除される移動局の情報を削除し、且つ該グループのうちの共有するグループ暗号通信用秘密鍵の更新、記憶を行った上、更新されたグループ所属移動局の個別秘密鍵で暗号化されたグループ暗号通信用秘密鍵を前記複数の移動局へ配送することを特徴とする移動通信システム。

【請求項6】 請求項1～5の何れか一つに記載の移動通信システムにおいて、前記データベースは、前記グループ暗号通信用秘密鍵を記憶、更新する毎に該秘密鍵に対応した識別情報を生成記憶し、前記制御局は、前記グループ暗号通信用秘密鍵の配送時に前記移動局個別の秘密鍵で暗号化された該グループ暗号通信用秘密鍵及び前記識別情報を配送すると共に、グループ通信要求が生じる毎に前記暗号化したグループ暗号通信用秘密鍵の代わりに前記識別情報を送付し、前記複数の移動局は、自局用の個別秘密鍵、自局が所属するグループで共有する前記グループ暗号通信用秘密鍵、及び該秘密鍵に対応した識別情報を記憶し、グループ通信生起時に前記制御局から送付された前記識別情報と自局内に記憶されている前記識別情報とを比較した結果、一致している場合には自局に記憶されている前記グループ暗号通信用秘密鍵を用いて暗号通信を行い、不一致の場合には前記制御局に対して前記データベースに記憶されている前記移動局個別の暗号鍵で暗号化された前記グループ暗号通信用秘密鍵の配送を要求することを特徴とする移動通信システム。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】本発明は、主として複数の移動局間でグループを構成して排他的なグループ秘話通信が可能な移動通信システムであって、詳しくは同一グループ内の移動局で共有する暗号通信用の秘密鍵を安全に管理し、且つ同一グループに所属する移動局に安全に配送することにより、同一グループ内の移動局間での秘話通信を行う移動通信システムに関する。

【0002】

【従来の技術】従来、この種の移動通信システムにおける秘話通信では、無線を利用したシステム特有の電波傍受に対する防止策として、基地局及び移動局間の通信を暗号化する手法が導入されている。例えば特開平3-203431号公報には、暗号技術により移動局個別の秘密鍵をセンタ交換局（制御局及びデータベースの機能を合わせたもの）が安全に蓄積管理すると共に、このセンタ交換局から移動局が在圏する基地局に該移動局の秘密鍵を安全に配送する技術が開示されている。

【0003】ところが、この手法の場合、秘密鍵の配送に際して暗号技術を適用し、基地局から制御局間の通信路の安全性を確保している（即ち、基地局から制御局間の伝送路での情報漏洩の可能性が考慮されている）にも

3

拘らず、通信安全性に対する配慮が払われていないことにより、複数の移動局でグループを構成してグループ内のそれぞれの移動局が暗号通信用の秘密鍵を共有して暗号通信を行うグループ秘話通信への適用は困難であるという問題がある。

【0004】そこで、複数のユーザ間でグループ秘話通信を行う手法として、同一グループ内のそれぞれのユーザが暗号通信用の秘密鍵を共有することにより排他的な秘話通信を行う技術が提案されている。例えば特開平4-38029号公報には、グループに所属するユーザのそれぞれが所属全ユーザのID情報を保持しておき、この全ユーザのID情報から生成したグループ共通鍵によりグループ内の暗号通信に使用する秘密鍵を暗号化してそれぞれのユーザに配送することにより、グループ暗号通信用秘密鍵を共有する技術が開示されている。

【0005】

【発明が解決しようとする課題】上述した既成のグループ秘話通信の場合、それぞれの移動局において、配送される暗号化されたグループ暗号通信用秘密鍵を復号化するためのグループ共通鍵を生成するために、グループ所属の全移動局のIDを記憶保持しておく必要があるため、第1の問題点としてグループ秘話通信のために移動局が記憶管理すべき情報量が多くなってしまう点が挙げられる。即ち、移動通信システムにおける移動局は、小型化や携帯性の向上に対する要求と、高機能化による情報端末化への要求とが高くなっており、こうした事情からも暗号秘話通信のために記憶管理すべき情報量は極力少なくすることが望まれているので、移動局が記憶管理すべき情報量が多い構成は不利なものとなっている。

【0006】又、既成のグループ秘話通信の場合、それぞれの移動局はグループ所属の全移動局のIDを記憶保持しておく必要があるため、グループ構成が変更される毎に所属グループの全移動局のID情報の配布を受ける必要があるが、このID情報がグループ外の第三者に漏洩することにより第三者によるグループ共通鍵の生成が可能になることを対策し、グループを構成する移動局のID情報をそれぞれの移動局に配送する場合には別の暗号通信により暗号化して無線回線を介して配送するか、或いは無線回線以外の安全な配送手段を用いる必要があるため、第2の問題点としてグループ構成の変更を容易に行うことができないという点が挙げられる。即ち、移動通信システムにおいては、広い地域に分散している移動局のグループ構成を無線回線を介して容易に変更することが求められるが、こうした場合にグループ通信の傍受に対する安全性を損なう可能性を回避することが望まれているので、グループ構成の変更を容易に行うことができない構成は不便なものとなっている。

【0007】更に、既成のグループ秘話通信の場合、受信端末（移動通信システムの移動局）の動作状態やグループ暗号通信用秘密鍵を安全に保管管理する機能が無い

4

ため、第3の問題点としてグループ秘話通信開始時に電源をオフにしていたり、或いは該当移動通信システムのサービスエリア外で通話不可状態にあったグループ所属移動局に対し、該当移動局が通話可能状態になった時点でもグループ秘話通信へ途中参加できないという不便が挙げられる。

【0008】本発明は、このような問題点を解決すべくなされたもので、その技術的課題は、複数の移動局でグループを構成して排他的なグループ秘話通信を具現し得る移動通信システムを提供することにある。

【0009】又、本発明の他の技術的課題は、グループ秘話通信の安全性を損なうことなく、グループ構成の変更が容易に可能な移動通信システムを提供することにある。

【0010】更に、本発明の別の技術的課題は、グループ通信開始時に電源オフ等により通話不可能状態であった移動局に対し、グループ秘話通信への途中参加を可能とする移動通信システムを提供することにある。

【0011】

【課題を解決するための手段】本発明によれば、呼接続を含む通信制御に必要な通信制御情報を記憶するデータベースと、通信制御情報に基づいて通信制御を行う制御局とを備えると共に、該制御局の通信制御に従って無線回線を介してそれぞれ複数の基地局と複数の移動局とを組み合わせることで通信接続することにより、該複数の移動局間でグループを構成して排他的なグループ秘話通信が可能な移動通信システムであって、データベースは、移動局個別情報として移動局個別の秘密鍵を内部のマスタ鍵で暗号化して記憶すると共に、グループ関連情報として所属移動局毎にグループ内で共有するグループ暗号通信用秘密鍵を該移動局個別の秘密鍵で暗号化して記憶し、制御局は、新規にグループ構成が行われる毎に該当グループに所属する移動局に対して暗号化したグループ暗号通信用秘密鍵を配送し、複数の移動局は、データベースに記憶されている移動局個別の秘密鍵のうちの自局用の秘密鍵を記憶すると共に、該当秘密鍵を用いて制御局より配送された暗号化されたグループ暗号通信用秘密鍵を復号化した上、該復号化されたグループのうちの共有するグループ暗号通信用秘密鍵を用いてグループ通信情報を暗号化、復号化する移動通信システムが得られる。

【0012】又、本発明によれば、上記移動通信システムにおいて、複数の移動局は、それぞれ自局の動作状態を複数の基地局のうちの特定のものと及び制御局を介してデータベースへ通報し、データベースは、通報された複数の移動局のそれぞれの動作状態情報を移動局個別情報として記憶し、制御局は、グループ暗号通信用秘密鍵の配送時に該当秘密鍵を受信不能であった該当グループ所属の移動局が受信可能状態になった場合、該グループ暗号通信用秘密鍵としてデータベースにおける移動局個別情報に従って該当移動局の秘密鍵で暗号化されたものを

配送する移動通信システムが得られる。

【0013】更に、本発明によれば、上記何れかの移動通信システムにおいて、データベースは、グループ暗号通信用秘密鍵として同一グループ内で共有するものを定期的に更新管理する移動通信システムが得られる。

【0014】これらの移動通信システムにおいて、データベースは、既設グループに所属移動局の追加を行う場合、該当グループへの新規加入移動局の個別移動局情報として記憶されている該当移動局の個別秘密鍵で該当グループのうちの共有するグループ暗号通信用秘密鍵を暗号化してグループ関連情報として記憶し、且つ該グループ暗号通信用秘密鍵を制御局及び複数の基地局のうちの対応するものを介して配送することや、或いはデータベースは、既設グループに所属移動局の一部削除を行う場合、該当グループ関連情報より削除される移動局の情報を削除し、且つ該当グループのうちの共有するグループ暗号通信用秘密鍵の更新、記憶を行った上、更新されたグループ所属移動局の個別秘密鍵で暗号化されたグループ暗号通信用秘密鍵を複数の移動局へ配送することは好ましい。

【0015】又、これらの移動通信システムにおいて、データベースは、グループ暗号通信用秘密鍵を記憶、更新する毎に該当秘密鍵に対応した識別情報を生成記憶し、制御局は、グループ暗号通信用秘密鍵の配送時に移動局個別の秘密鍵で暗号化された該当グループ暗号通信用秘密鍵及び識別情報を配送すると共に、グループ通信要求が生起する毎に暗号化したグループ暗号通信用秘密鍵の代わりに識別情報を送付し、複数の移動局は、自局用の個別秘密鍵、自局が所属するグループで共有するグループ暗号通信用秘密鍵、及び該当秘密鍵に対応した識別情報を記憶し、グループ通信生起時に制御局から送付された識別情報と自局内に記憶されている識別情報とを比較した結果、一致している場合には自局に記憶されているグループ暗号通信用秘密鍵を用いて暗号通信を行い、不一致の場合には制御局に対してデータベースに記憶されている移動局個別の暗号鍵で暗号化されたグループ暗号通信用秘密鍵の配送を要求することは好ましい。

【0016】

【発明の実施の形態】以下に実施例を挙げ、本発明の移動通信システムについて、図面を参照して詳細に説明する。

【0017】図1は、本発明の一実施例に係る移動通信システムの基本構成を示したブロック図である。この移動通信システムは、自局の認証や個別の暗号秘話通信等に使用される移動局個別秘密鍵 $k_1 \sim k_m$ 、自局が所属するグループを識別する番号 $G_1 \sim G_j$ 、及び同一グループ内で自局で共有するグループ暗号通信用の秘密鍵 $G_{k_1} \sim G_{k_j}$ を記憶した複数の移動局 $(MS_1 \sim MS_m)$ $40_1 \sim 40_m$ と、これらの移動局 $(MS_1 \sim MS_m)$ $40_1 \sim 40_m$ のうちの自局の無線ゾーンに在圏す

るものと無線回線を介して接続された複数の基地局 $(BS_1 \sim BS_n)$ $30_1 \sim 30_n$ と、所属する全ての移動局 $(MS_1 \sim MS_m)$ $40_1 \sim 40_m$ の情報を通信制御情報に含んで管理する記憶装置であって、通信制御情報として移動局 $(MS_1 \sim MS_m)$ $40_1 \sim 40_m$ のそれぞれの基地局 $(BS_1 \sim BS_n)$ $30_1 \sim 30_n$ における在圏位置情報、内部のマスタ鍵で暗号化された移動局個別の秘密鍵、移動局 $(MS_1 \sim MS_m)$ $40_1 \sim 40_m$ のそれぞれが所属するグループの番号等の移動局個別情報、並びにシステム内グループ構成やグループ暗号通信用秘密鍵等のグループ関連情報を記憶管理するデータベース10と、基地局 $(BS_1 \sim BS_n)$ $30_1 \sim 30_m$ と有線又は無線回線を介して接続され、データベース10の情報に従って呼接続制御を行う制御局20とから成っている。

【0018】この移動通信システムでは、同一グループ G_1 を構成する移動局 (MS_1, MS_2, MS_m) $40_1, 40_2, 40_m$ がグループ暗号通信用秘密鍵 G_{K_1} を使用して情報を暗号化することでグループ秘話通信を行う。ここでは、例えば移動局 (MS_1, MS_2) $40_1, 40_2$ が同じ通話チャネル1(CH1)を介して無線基地局 (BS_1) 30_1 に接続されると共に、移動局 (MS_m) 40_m が通話チャネル t (CH t)を介して無線基地局 (BS_n) 30_n に接続され、通話チャネル1と通話チャネル t とがそれぞれ基地局 (BS_1, BS_n) $30_1, 30_n$ を介して制御局20において相互に接続されることにより、グループ G_1 の秘話通信が行われることを示している。尚、図1中において、基地局 $(BS_1 \sim BS_n)$ $30_1 \sim 30_n$ に関しては基地局 (BS_1, BS_2, BS_n) $30_1, 30_2, 30_n$ 以外の局が省略され、移動局 $(MS_1 \sim MS_m)$ $40_1 \sim 40_m$ に関しては移動局 (MS_1, MS_2, MS_i, MS_m) $40_1, 40_2, 40_i, 40_m$ (但し、 $m > i$ とする)以外の局が省略されている。

【0019】このうち、データベース10は、移動局個別情報として移動局個別の秘密鍵を内部のマスタ鍵で暗号化して記憶すると共に、グループ関連情報として所属移動局毎にグループ内で共有するグループ暗号通信用秘密鍵を該移動局個別の秘密鍵で暗号化して記憶する。制御局20は、新規にグループ構成が行われる毎に該当グループに所属する移動局に対して暗号化したグループ暗号通信用秘密鍵を配送する。複数の移動局 $(MS_1 \sim MS_m)$ $40_1 \sim 40_m$ は、データベース10に記憶されている移動局個別の秘密鍵のうちの自局用の秘密鍵を記憶すると共に、該当秘密鍵を用いて制御局20より配送された暗号化されたグループ暗号通信用秘密鍵を復号化した上、復号化されたグループのうちの共有するグループ暗号通信用秘密鍵を用いてグループ通信情報を暗号化、復号化する。

【0020】即ち、こうした場合の移動通信システムで

は、データベース10には移動局個別情報として在圏位置情報、所属グループのグループ番号、及び移動局の認証や個別秘話通信等に使用される移動局個別の秘密鍵を内部のマスタ鍵で暗号化して記憶すると共に、グループ関連情報として移動局個別情報の内容とリンクして所属移動局番号、該当移動局の在圏位置情報、及びグループ暗号通信用秘密鍵を移動局個別の暗号鍵で暗号化して記憶しておくことにより、システム内で使用する暗号秘話通信用の鍵を安全に記憶管理することができ、且つ同一グループに所属する移動局へのグループ暗号通信用秘密鍵の配送時にも配送先移動局の個別暗号鍵で暗号化された情報を配送しているため、複数の移動局(MS1~MSm)40₁~40_m間でグループを構成して排他的なグループ秘話通信を安全且つ容易に行うことができる。

【0021】一方、この移動通信システムにおいて、複数の移動局(MS1~MSm)40₁~40_mは、それぞれ自局の動作状態を複数の基地局(BS1~BSn)30₁~30_nのうちの特定のものと及び制御局20を介してデータベース10へ通報する。データベース10は、通報された複数の移動局(MS1~MSm)40₁~40_mのそれぞれの動作状態情報を移動局個別情報として記憶する。制御局20は、グループ暗号通信用秘密鍵の配送時に該当秘密鍵を受信不能であった該当グループ所属の移動局が受信可能状態になった場合、グループ暗号通信用秘密鍵としてデータベース10における移動局個別情報に従って該当移動局の秘密鍵で暗号化されたものを配送する。

【0022】こうした場合の移動通信システムでは、グループ秘話通信開始時に電源オフやシステムのサービスエリア外にあって該当グループ秘話通信に参加できなかったグループ所属の移動局があった場合にも、その移動局が新たに在圏位置登録等を行うことで、制御局20がグループ通信へ参加可能な状態になったと判明した場合にデータベース10の情報に従って、該当移動局の秘密鍵で暗号化されたグループ暗号通信用秘密鍵を配送することにより、グループ秘話通信への途中参加が可能になる。

【0023】他方、この移動通信システムにおいて、データベース10は、グループ暗号通信用秘密鍵として同一グループ内で共有するものを定期的に更新管理するが、既設グループに所属移動局の追加を行う場合には該当グループへの新規加入移動局の個別移動局情報として記憶されている該当移動局の個別秘密鍵で該当グループのうちの共有するグループ暗号通信用秘密鍵を暗号化してグループ関連情報として記憶し、且つそのグループ暗号通信用秘密鍵を制御局20及び複数の基地局(BS1~BSn)30₁~30_nのうちの対応するものを介して配送し、既設グループに所属移動局の一部削除を行う場合には該当グループ関連情報より削除される移動局の情報を削除し、且つ該当グループのうちの共有するグル

ープ暗号通信用秘密鍵の更新、記憶を行った上、更新されたグループ所属移動局の個別秘密鍵で暗号化されたグループ暗号通信用秘密鍵を複数の移動局(MS1~MSm)40₁~40_mへ配送する。

【0024】こうした場合の移動通信システムでは、データベース10において、グループ関連情報が移動局個別情報とリンクして記憶管理され、システム内の暗号鍵関連情報が安全に記憶管理されているため、データベース10内でのグループ構成の変更が安全且つ容易に可能であり、システム構成の変更に伴う移動局へのグループ暗号通信用秘密鍵の関連情報が安全に配送できる。このため、グループ秘話通信の安全性を損なうことなく、グループ所属移動局の増減等のグループ構成の変更が容易に可能となる。

【0025】図2は、この移動通信システムに備えられるデータベース10の内容を例示したものである。

【0026】このデータベース10は、移動通信システムにおいてm台の移動局(MS1~MSm)40₁~40_mが所属し、更にそれぞれの移動局(MS1~MSm)40₁~40_mがシステム内に構成されているj個のグループG1~Gjに所属していることを示している。即ち、データベース10には移動局個別情報として、それぞれの移動局(MS1~MSm)40₁~40_mの移動局番号に対応して該当局が所属するグループ番号G1~Gjと、それぞれの自局の認証や移動局個別の暗号秘話通信等に使用される移動局個別秘密鍵k1~kmを内部のマスタ鍵kMで暗号化した個別秘密鍵情報E(K1, kM)~E(km, kM)と、それぞれの自局の基地局(BS1~BSn)30₁~30_nにおける在圏位置情報として在圏基地局番号BS1~BSnとが記憶されている。又、データベース10にはグループ関連情報として、移動局個別情報をグループ番号単位にまとめて再記憶したグループG1~Gj毎の所属移動局番号及び該当局の在圏基地局番号と、それぞれのグループのグループ暗号通信用秘密鍵Gk1~Gkjをグループに所属するそれぞれの移動局(MS1~MSm)40₁~40_mの個別暗号通信用秘密鍵k1~kmで各々暗号化したグループ暗号通信用秘密鍵情報E(Gk1, k1)~E(Gkj, km)とが記憶されている。

【0027】このデータベース10では、移動局(MS1~MSm)40₁~40_mより位置登録要求が行われる毎に該当局の移動局個別情報の中の在圏基地局番号が書き換えられると共に、該当局に対応したグループ関連情報の書き換えが行われる。又、既設のグループで所属移動局の増減によるグループ構成の変更が行われる場合、データベース10は所属移動局が増えるグループに対しては該当グループ情報の記憶エリアに追加移動局の移動局番号、移動局個別情報として記憶されている該当移動局の在圏位置情報、及び移動局に対応したグループ暗号通信用秘密鍵情報を追加記憶すると共に、該当移動

局に対しては制御局20及び移動局が在圏する基地局を介して変更されたグループ番号等の情報を配送する。尚、データベースに変更記憶される追加移動局のグループ暗号通信用秘密鍵情報は、移動局個別情報として内部のマスタ鍵 kM で暗号化されて記憶されている該当移動局の個別秘密鍵 K^* （*は移動局の番号情報を示す）をマスタ鍵 kM で復号化し、復号化された個別秘密鍵 k^* でグループ暗号通信用の秘密鍵 Gk^{**} （**はグループの番号情報を示す）を暗号化するようにして内部で作成する。

【0028】因みに、データベース10では、上述したように所属移動局が削減されるグループに対して該当グループ関連情報より削除される移動局の情報を削除すると共に、該当グループのグループ暗号通信用秘密鍵の更新を行うことにより、グループ秘話通信の安全性を損なうことなく容易にグループ構成の変更を行うことができるようになっている。

【0029】図3は、図2に示したデータベース10を用いた場合の移動通信システムによるグループ秘話通信の呼接続シーケンスを示したものである。

【0030】ここでは、先ず移動局（ $MS1$ ） 40_1 が自身の所属するグループ $G1$ 内でグループ秘話通信を行うために呼接続シーケンスを $G1$ 発呼として基地局（ $BS1$ ） 30_1 へ発呼し、グループ $G1$ に対して行われた $G1$ 発呼の情報は基地局（ $BS1$ ） 30_1 を介して制御局20に送られ、ここでデータベース10に対して $G1$ 関連情報の問合せが行われる。問合せを受けたデータベース10は、グループ $G1$ に対応した図2に示した在圏基地局番号を読み出すことにより、グループ $G1$ に所属する移動局が在圏する基地局番号を $G1$ 在圏位置情報として制御局20へ報告すると共に、所属移動局毎の個別暗号通信用秘密鍵で暗号化されたグループ暗号通信用秘密鍵情報を制御局20へ送出する。

【0031】制御局20は、報告を受けた全ての在圏基地局に対してグループ $G1$ への $G1$ 着呼を通知すると共に、それぞれの基地局に在圏する該当グループ所属移動局向けのグループ暗号通信関連情報としてグループ暗号通信用秘密鍵情報 $E(Gk1, k1)$ 、 $E(Gk1, k2)$ の配送を行う。尚、制御局20は基地局（ BSn ） 30_n に対して $G1$ 着呼及びグループ暗号通信用秘密鍵情報 $E(Gk1, km)$ を送信する。グループ $G1$ への $G1$ 着呼通知を受けた基地局（ $BS1$ ） 30_1 は無線ゾーンにおいてグループ $G1$ に対する通話チャンネル（ CH ）割当、グループ暗号通信用秘密鍵情報 $E(Gk1, k1)$ 、 $E(Gk1, k2)$ 配送、及び $G1$ 着信呼出を行う。尚、このとき、制御局20から $G1$ 着呼及びグループ暗号通信用秘密鍵情報 $E(Gk1, km)$ を受けた基地局（ BSn ） 30_n は、通話チャンネル（ CH ）割当、グループ暗号通信用秘密鍵情報 $E(Gk1, km)$ 配送、及び $G1$ 着信呼出を行う。

【0032】制御局20からグループ暗号通信用秘密鍵情報の配送を受けた移動局（ $MS1$ 、 $MS2$ 、 MSm ） 40_1 、 40_2 、 40_m は、自身が記憶管理している移動局個別秘密鍵によりグループ暗号通信用秘密鍵 $Gk1$ を復号化し、該当秘密鍵 $Gk1$ で平文情報 M を暗号化した情報 $E(M, Gk1)$ を受け渡しすることによりグループ秘話通信を行う。

【0033】図4は、図2に示すデータベース10を使用して図3に示す呼接続シーケンスにおいて、基地局（ $BS1$ 、 BSn ） 30_1 、 30_n から移動局（ $MS1$ 、 $MS2$ 、 MSm ） 40_1 、 40_2 、 40_m へグループ暗号通信用秘密鍵情報を配送する場合の信号構成例を示したもので、同図（a）は基地局（ $BS1$ ） 30_1 から該当局の無線ゾーンに在圏する移動局（ $MS1$ 、 $MS2$ ） 40_1 、 40_2 等へ配送する場合に関するもの、同図（b）は基地局（ BSn ） 30_n から移動局（ MSm ） 40_m 等へ配送する場合に関するものである。

【0034】ここでは、上述したデータベース10では、それぞれのグループ所属移動局の在圏位置情報が記憶管理されているため、基地局（ $BS1 \sim BSn$ ） $30_1 \sim 30_n$ での情報伝送量を最小限に押さえ得ることを示唆している。

【0035】図5は、この移動通信システムに適用可能な図2に示すデータベース10とは他のデータベース10'を例示したものである。このデータベース10'におけるデータベース10との相違は、グループ関連情報としてそれぞれのグループのグループ暗号通信用秘密鍵のバージョンに対応したグループ暗号通信用秘密鍵の識別情報を記憶するようにした点にある。通信傍受や暗号解読に対する安全性を確保する観点や、所属していた移動局が別のグループに移った等によりグループ構成が変更された場合等に際し、グループ暗号通信用の秘密鍵は、定期的或いは不定期に更新変更を行う必要がある。

【0036】この更新変更に対応したそれぞれのグループ暗号通信用秘密鍵のバージョン情報としてのグループ暗号通信用秘密鍵識別情報を記憶管理し、鍵更新時に所属移動局へ、更新された鍵（図2の場合と同様にそれぞれの移動局の個別暗号通信用秘密鍵で暗号化されたグループ暗号通信用秘密鍵）とこれに対応したグループ暗号通信用秘密鍵識別情報 $IGk1 \sim IGkj$ とを配送する。これにより、鍵更新時以外のグループ呼接続時等ではグループ番号に対応したグループ暗号通信用秘密鍵識別情報 $IGk1 \sim IGkj$ を送付するのみで、図4に示した移動局毎のグループ暗号通信用秘密鍵情報を配布する必要を排除できる。尚、図5において移動局個別情報に関しては図2と同一であるために略図している。

【0037】図6は、図5によるデータベース10'を使用した場合、グループ呼接続時に該当グループに所属する移動局が在圏するそれぞれの基地局から移動局へ配送されるグループ暗号通信用の秘密鍵に関連する情報と

して、その信号構成を例示したものである。

【0038】ここでは、グループ暗号通信用秘密鍵のバージョン情報としてのグループ暗号通信用秘密鍵識別情報を配送するため、それぞれの基地局に在圏する移動局に対応して配送情報を変更する必要が無く、又グループ暗号通信用秘密鍵識別情報が、更新前の鍵の誤使用を防ぐのが目的となっているため、比較的短いシーケンシャルな数字や鍵更新時の日付等を使用することができるようになっている。これにより、データベース10を使用した場合のグループ暗号通信用秘密鍵情報の配送に比

べ、グループ呼接続時の配送情報量の大幅な削減や周波数利用効率の向上を計り得るようになっている。

【0039】図7は、本発明の他の実施例に係る移動通信システムによるグループ暗号通信の呼接続シーケンスを示したものである。ここでのグループ秘話通信の呼接続シーケンスは、図1に示した移動通信システムにおいて、グループ呼が生起し、呼接続が行われる時点で電源オフや、システムのサービス圏外にいた該当グループ所属の移動局がサービスを受けられる状態になった場合、途中から該当グループ秘話通信に参加することを可能とするものである。

【0040】即ち、ここでは図3に示すシーケンスに加えて新たな処理手順が追加されているが、ここでの移動局(MSm)40_mはグループG1のグループ秘話通信開始時まで電源がオフになっており、グループ秘話通信に参加できていない状態を示している。

【0041】そこで、図7を参照すれば、電源をオンした移動局(MSm)40_mは自局が在圏する基地局(BSn)30_nを介して制御局20に対して位置登録要求を行い、基地局(BSn)30_nから制御局20へMSm位置登録要求を行う。移動局(MSm)40_mからのMSm位置登録要求を受けた制御局20は、データベース10に対して移動局(MSm)40_mのMSm位置登録情報を送付し、送付を受けたデータベース10は個別移動局情報及びグループ関連情報の在圏基地局番号の書き換えを行ってMSm位置登録すると共に、MSm位置登録を行った移動局(MSm)40_m関連のMSm関連情報及びグループ暗号通信用秘密鍵情報E(Gk1, km)を制御局20へ送付する。

【0042】制御局20では、データベース10より送付されたMSm関連情報から該当局の所属グループ番号と現在通話中のグループ番号とを照合し、このグループが通話中の場合にはデータベース10より該当グループのグループ暗号通信用秘密鍵情報を入手し、移動局(MSm)40_mが在圏する基地局(BSn)30_nに対して移動局(MSm)40_mへのMSm着呼を通知すると共に、グループ暗号通信用秘密鍵情報E(Gk1, km)を送付する。送付を受けた基地局(BSn)30_nは、該当グループ通信へ通話チャネル(CH)が割り当てられていない場合には通話チャネル(CH)割当を行

うと共に、グループ暗号通信用秘密鍵情報E(Gk1, km)の配送及びグループG1のG1着信呼を行う。これにより、移動局(MSm)40_mはグループ暗号鍵Gk1を使用したグループ秘話通信に参加できることになる。

【0043】尚、図7ではデータベース10を使用した場合について説明したが、図中のグループ暗号通信用秘密鍵情報をグループ暗号通信用秘密鍵識別情報に置き換えれば、図5に示すデータベース10'も適用することができ、データベース10'を使用した場合も同様な効果が得られる。具体的に云えば、このような構成の移動通信システムにおいて、データベース10'は、グループ暗号通信用秘密鍵を記憶、更新する毎に該当秘密鍵に対応した識別情報を生成記憶する。制御局20は、グループ暗号通信用秘密鍵の配送時に移動局個別の秘密鍵で暗号化された該当グループ暗号通信用秘密鍵及び識別情報を配送すると共に、グループ通信要求が生起する毎に暗号化したグループ暗号通信用秘密鍵の代わりに識別情報を送付する。複数の移動局(MS1~MSm)40₁~40_mは、自局用の個別秘密鍵、自局が所属するグループで共有するグループ暗号通信用秘密鍵、及び該当秘密鍵に対応した識別情報を記憶し、グループ通信生起時に制御局から送付された識別情報と自局内に記憶されている識別情報とを比較した結果、一致している場合には自局に記憶されているグループ暗号通信用秘密鍵を用いて暗号通信を行い、不一致の場合には制御局20に対してデータベース10'に記憶されている移動局個別の暗号鍵で暗号化されたグループ暗号通信用秘密鍵の配送を要求する。

【0044】即ち、こうした場合の移動通信システムでは、データベース10'において、在圏位置情報等の移動局の動作状態がグループ関連情報とリンクして記憶管理されているため、グループ秘話通信開始時に電源オフ等により通話可能状態になかった移動局が通話可能な状態になる。そこで、データベース10'は、新たに在圏位置登録等を行った場合には該当移動局の所属グループ番号等のグループ関連情報を制御局20に送付し、送付を受けた制御局20は該当移動局所属のグループ番号と現在通話中のグループ番号を照合し、グループが秘話通話中の場合には該当移動局に対してグループ暗号通信用秘密鍵を送付するため、通話中のグループ秘話通信への途中参加が可能となる。

【0045】

【発明の効果】以上に述べた通り、本発明の移動通信システムによれば、制御局により複数の基地局のうちの特定なもの及び複数の移動局の組み合わせ間における通信制御に際して使用する通信制御情報を記憶するデータベースに関して、移動局個別情報として在圏位置情報、所属グループのグループ番号、及び移動局の認証や個別秘話通信等に使用される移動局個別の秘密鍵を内部のマス

タ鍵で暗号化して記憶すると共に、グループ関連情報として所属移動局番号、該当移動局の在圏位置情報、及びグループ暗号通信用秘密鍵をそれぞれの移動局の個別秘密鍵で暗号化した情報を記憶することにより、システム内で使用する暗号秘話通信用の鍵を安全に記憶管理することができ、複数の移動局でグループを構成して排他的なグループ秘話通信を安全且つ容易に実行することができるようになる。その理由は、データベースにおいて移動局個別の秘密鍵は内部のマスタ鍵で暗号化して記憶され、グループ暗号通信用秘密鍵はそれぞれ移動局毎に移動局個別秘密鍵で暗号化されて記憶管理されるため、万一データベースの情報が漏れても暗号関連の鍵が盗まれる心配が無い上、所属移動局へのグループ暗号通信用秘密鍵の配送時にも配送先各移動局の個別秘密鍵で暗号化された情報が配送されることによる。

【0046】又、この移動通信システムの場合、データベースにおいて、グループ関連情報が移動局個別情報とリンクして記憶管理されており、又システム内の暗号鍵関連情報が安全に記憶管理されているため、データベース内でのグループ構成の変更が安全且つ容易なことや、システム構成の変更に伴う移動局へのグループ暗号通信用秘密鍵関連情報が安全に配送できることにより、グループ秘話通信の安全性を損なうことなく、グループ所属移動局の増減等のグループ構成の変更が容易に可能となる。

【0047】更に、この移動通信システムの場合、データベースにおいて、在圏位置情報等の移動局の動作状況がグループ関連情報とリンクして記憶管理されているため、グループ秘話通信開始時に電源オフ等により通話可

能状態に無かった移動局に対し、グループ秘話通信への途中参加を可能とすることができるようになる。

【図面の簡単な説明】

【図1】本発明の一実施例に係る移動通信システムの基本構成を示したブロック図である。

【図2】図1に示す移動通信システムに備えられるデータベースの内容を例示したものである。

【図3】図1に示す移動通信システムによるグループ秘話通信の呼接続シーケンスを示したものである。

10 【図4】図2に示すデータベースを使用して図3に示す呼接続シーケンスにおいて、基地局から移動局へグループ暗号通信用秘密鍵情報を配送する場合の信号構成を例示したもので、(a)は特定の基地局から該当局の無線ゾーンに在圏する特定の移動局等へ配送する場合に関するもの、(b)は他の基地局から他の移動局等へ配送する場合に関するものである。

【図5】図2に示すデータベースの他の形態によるデータベースの内容を例示したものである。

20 【図6】図5に示すデータベースを使用した場合のグループ暗号通信用秘密鍵配送時の信号構成を例示したものである。

【図7】本発明の他の実施例に係る移動通信システムによるグループ暗号通信の呼接続シーケンスを示したものである。

【符号の説明】

10、10' データベース

20 制御局

30₁ ~ 30_n 基地局 (BS₁ ~ BS_n)

40₁ ~ 40_m 移動局 (MS₁ ~ MS_m)

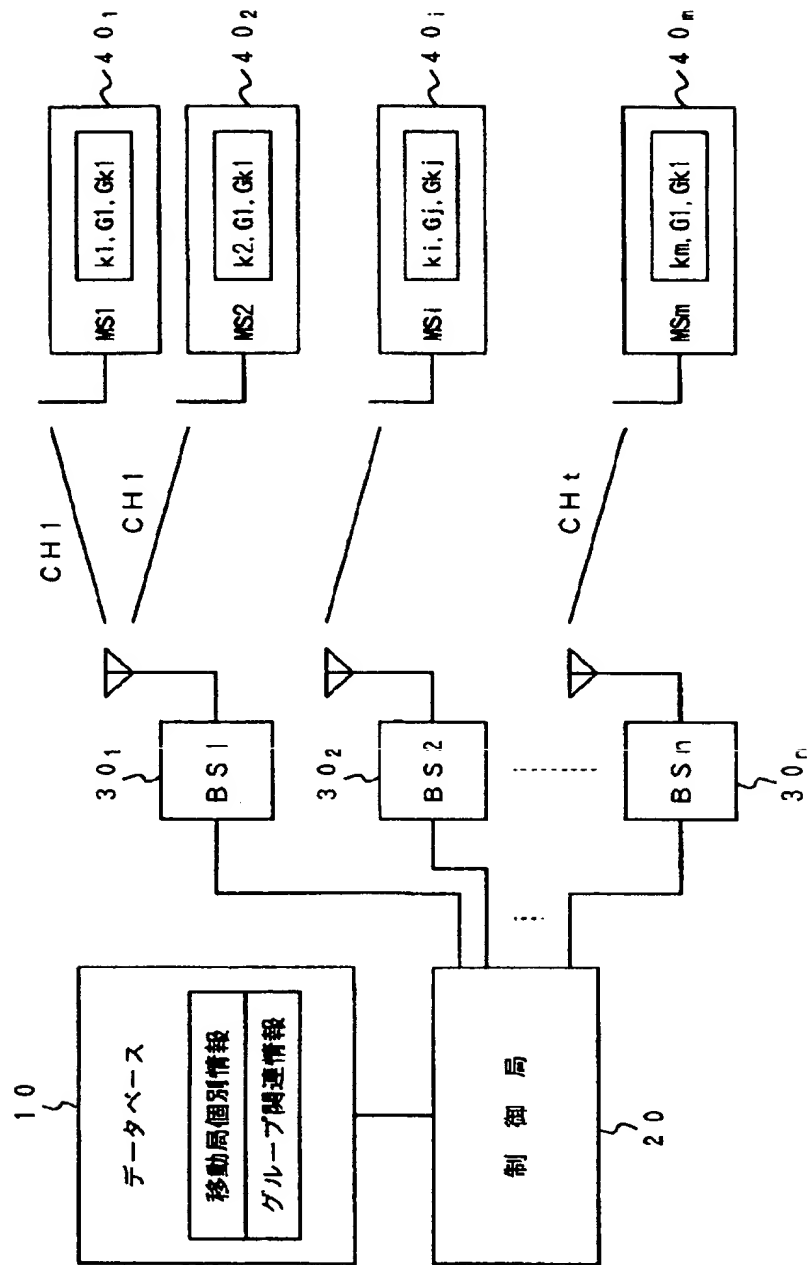
【図4】

(a)			
MS1	E (Gk1, k1)	MS2	E (Gk1, k2)
(b)			
MSm	E (Gk1, km)	

【図6】

グループ番号	グループ暗号通信用秘密鍵識別情報
G1	IGk1

【図1】



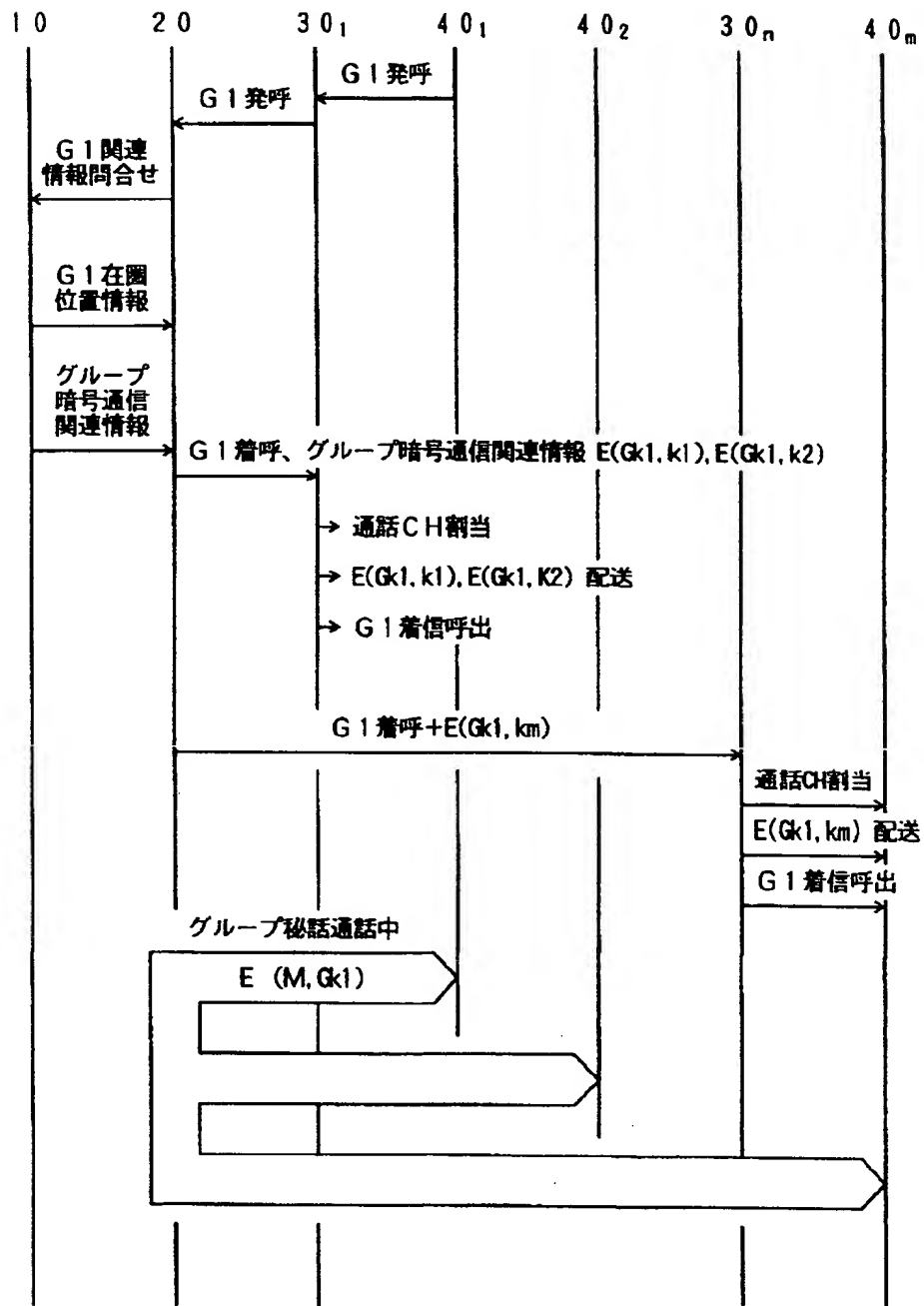
【図2】

10

5

データベース			
移動局個別情報			
移動局番号	所属グループ番号	個別秘密鍵情報	在圏基地局番号
MS 1	G 1	E (k1, kN)	BS 1
MS 2	G 1	E (k2, kN)	BS 1
⋮			
MS i	G j	E (ki, kN)	BS 2
⋮			
MS m	G 1	E (km, kN)	BS n
グループ関連情報			
グループ番号	グループ所属移動局関連情報		
G 1	MS 1	MS 2	⋯⋯⋯⋯⋯
	BS 1	BS 1	
	E (Gk1, k1)	E (Gk1, k2)	E (Gk1, km)
⋮			
G j	⋯⋯⋯⋯⋯	MS i	⋯⋯⋯⋯⋯
		BS 2	
		E (Gkj, ki)	

【図3】



【図5】

10'
S

データベース					
移動局個別情報					
⋮					
グループ関連情報					
グループ 番号	グループ暗号通信用 秘密鍵識別情報	グループ所属移動局関連情報			
G1	IGk1	MS1	MS2	MSm
		BS1	BS1		BSn
		E(Gk1, k1)	E(Gk1, k2)		E(Gk1, km)
⋮					
Gj	IGkj	MSi	
			BS2		
			E(Gkj, ki)		

D

**This Page is Inserted by IFW Indexing and Scanning
Operations and is not part of the Official Record**

BEST AVAILABLE IMAGES

Defective images within this document are accurate representations of the original documents submitted by the applicant.

Defects in the images include but are not limited to the items checked:

- ☐ BLACK BORDERS
- ☐ IMAGE CUT OFF AT TOP, BOTTOM OR SIDES
- ☐ FADED TEXT OR DRAWING
- ☐ BLURRED OR ILLEGIBLE TEXT OR DRAWING
- ☐ SKEWED/SLANTED IMAGES
- ☐ COLOR OR BLACK AND WHITE PHOTOGRAPHS
- ☐ GRAY SCALE DOCUMENTS
- ☒ LINES OR MARKS ON ORIGINAL DOCUMENT
- ☐ REFERENCE(S) OR EXHIBIT(S) SUBMITTED ARE POOR QUALITY
- ☐ OTHER: _____

IMAGES ARE BEST AVAILABLE COPY.

As rescanning these documents will not correct the image problems checked, please do not report these problems to the IFW Image Problem Mailbox.